Optimal Power Allocation for Secure Communications in Large-Scale MIMO Relaying Systems

Jian Chen†, Xiaoming Chen†, Xiumin Wang‡, and Lei Lei†
†College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, China.
‡School of Computer and Information, Hefei University of Technology, Hefei, China.
Email: chenxiaoming@nuaa.edu.cn

***Abstract*—In this paper, we address the problem of optimal power allocation at the relay in two-hop secure communications. In order to solve the challenging issue of short-distance interception in secure communications, the benefit of large-scale MIMO (LS-MIMO) relaying techniques is exploited to improve the secrecy performance significantly, even in the case without eavesdropper channel state information (CSI). The focus of this paper is on the analysis and design of optimal power allocation for the relay, so as to maximize the secrecy outage capacity. We reveal the condition that the secrecy outage capacity is positive, prove that there is one and only one optimal power, and present an optimal power allocation scheme. Moreover, the asymptotic characteristics of the secrecy outage capacity is carried out to provide some clear insights for secrecy performance optimization. Finally, simulation results validate the effectiveness of the proposed scheme.**

I. Introduction

Wireless security is always a critical issue due to the open nature of the wireless channel. Traditionally, high-layer encryption techniques are adopted to guarantee secure communications. However, information-theoretic study shows that the originally harmful factors of wireless channels, such as fading, noise and interference, can be used to realize wireless security, namely physical layer security [1] [2], then the complicated encryption can be partially replaced, especially in mobile communications.

It has been proved repeatedly that the secrecy performance is determined by the rate difference between the legitimate channel and the eavesdropper channel [3] [4]. To improve the secrecy performance, multi-antenna relaying techniques are commonly used in physical layer security [5]. On the one hand, the use of the relay shortens the access distance, and thus increases the legitimate channel rate. On the other hand, multi-antenna techniques can be applied to impair the interception signal. The beamforming schemes at the MIMO relay based on global channel state information (CSI) for amplify-and-forward (AF) and decode-and-forward (DF) relaying systems were presented in [6] and [7], respectively. Note that the beam design in secure communications requires both legitimate and eavesdropper CSI [8]. However, it is usually difficult to obtain eavesdropper CSI due to the well hidden property of the eavesdropper. In this context, the beam is not optimal, and thus the secrecy performance is degraded. To solve it, a joint jamming and beamforming scheme at the relay in the case without eavesdropper CSI was proposed in [9]. The relay transmits the artificial noise signal in the null space of the legitimate channel together with the forward signal, so the quality of the interception signal is weakened. This scheme improves the secrecy performance at the cost of power efficiency.

Recently, LS-MIMO relaying techniques are introduced into secure communications to improve the secrecy performance [10]. It is found that even without eavesdropper CSI, LS-MIMO techniques can produce a high-resolution spatial beam, then the information leakage to the eavesdropper is quite small. More importantly, the secrecy performance can be enhanced by simply adding the antennas. Thus, the challenging issue of short-distance interception in secure communications can be well solved. Note that in two-hop secure systems, the transmit power at the relay has a great impact on the secrecy performance, since the power will affect the signal quality at the destination and the eavesdropper simultaneously. An optimal power allocation scheme for a multi-carrier two-hop single-antenna relaying network was given by maximizing the sum secrecy rate in [11]. However, the power allocation for a multi-antenna relay, especially an LS-MIMO relay, is still an open issue. In this paper, we focus on power allocation for secure two-hop LS-MIMO relaying systems under very practical assumptions, i.e., no eavesdropper CSI and imperfect legitimate CSI. The contributions of this paper are three-fold:

1) We reveal the relation between the secrecy outage capacity and the defined relative distance-dependent path loss, and then give the condition that the secrecy outage capacity is positive.
2) We prove that there is one and only one optimal power at the relay, and propose an optimal power allocation scheme.
3) We present several clear insights for secrecy performance optimization through asymptotic analysis.

The rest of this paper is organized as follows. We first give an overview of the secure LS-MIMO relaying system in Section II, and then analyze and design an optimal power

allocation scheme for the relay in Section III. In Section IV, we present some simulation results to validate the effectiveness of the proposed scheme. Finally, we conclude the whole paper in Section V.

II. System Model

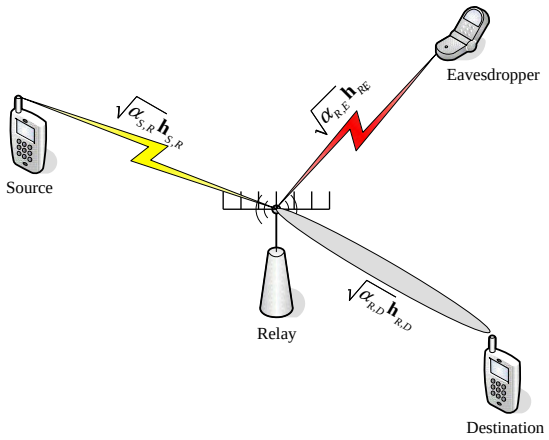

Fig. 1. An overview of a secure LS-MIMO relaying system.

Consider a time division duplex (TDD) two-hop LS-MIMO relaying system, as shown in Fig.1. It consists of one source, one destination and one passive eavesdropper, equipped with a single antenna each, and one relay with N_R antennas. It is worth pointing out that N_R is quite large in this LS-MIMO relaying system, i.e. $N_R = 100$ or larger. In addition, it is assumed that the distance between the source and the destination is so long that it is impossible to transmit the information from the source to the destination directly. The whole system works in a half-duplex mode, which means that a complete transmission requires two time slots. Specifically, in the first time slot, the source sends the signal to the relay, and then the relay forwards the post-processing signal to the destination during the second time slot. We assume that the eavesdropper is far away from the source and close to the relay, since it thought the signal comes from the relay. Then, the eavesdropper only monitors the transmission from the relay to the destination. Note that this is a common assumption in previous related literatures, because it is difficult for the eavesdropper to monitor both the source and the relay.

We use $\sqrt{\alpha_{S,R}}\mathbf{h}_{S,R}$, $\sqrt{\alpha_{R,D}}\mathbf{h}_{R,D}$ and $\sqrt{\alpha_{R,E}}\mathbf{h}_{R,E}$ to represent the channels from the source to the relay, the relay to the destination, and the relay to the eavesdropper respectively, where $\alpha_{S,R}$, $\alpha_{R,D}$ and $\alpha_{R,E}$ are the distance-dependent path losses and $\mathbf{h}_{S,R}$, $\mathbf{h}_{R,D}$, and $\mathbf{h}_{R,E}$ are channel small scale fading vectors with independent and identically distributed (i.i.d.) zero mean and unit variance complex Gaussian entries. It is assumed that the channels remain constant during a time slot and fade independently over slots. Thus, the received signal at the relay in the first time slot can be expressed as

$$\mathbf{y}_R = \sqrt{P_S \alpha_{S,R}}\mathbf{h}_{S,R} s + \mathbf{n}_R, \tag{1}$$

where s is the normalized Gaussian distributed transmit signal, P_S is the transmit power at the source, $\mathbf{n}_R$ is the additive Gaussian white noise with zero mean and unit variance at the relay.

Then, the relay adopts an amplify-and-forward (AF) relaying protocol to forward the received signal. Due to the low complexity and good performance in LS-MIMO systems, we combine maximum ratio combination (MRC) and maximum ratio transmission (MRT) at the relay to process the received signal. We further assume that the relay has perfect CSI about $\mathbf{h}_{S,R}$ by channel estimation and gets partial CSI about $\mathbf{h}_{R,D}$ due to channel reciprocity in TDD systems. The relation between the estimated CSI $\hat{\mathbf{h}}_{R,D}$ and the real CSI $\mathbf{h}_{R,D}$ is given by

$$\mathbf{h}_{R,D} = \sqrt{\rho}\hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho}\mathbf{e}, \tag{2}$$

where $\mathbf{e}$ is the error noise vector with i.i.d. zero mean and unit variance complex Gaussian entries, and is independent of $\hat{\mathbf{h}}_{R,D}$. ρ, scaling from 0 to 1, is the correlation coefficient between $\hat{\mathbf{h}}_{R,D}$ and $\mathbf{h}_{R,D}$. Then, the normalized signal to be transmitted at the relay can be expressed as

$$\mathbf{r}^{AF} = \mathbf{F}\mathbf{y}_R, \tag{3}$$

where $\mathbf{F}$ is the processing matrix, which is given by

$$\mathbf{F} = \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \frac{1}{\sqrt{P_S \alpha_{S,R}\|\mathbf{h}_{S,R}\|^2 + 1}} \frac{\mathbf{h}_{S,R}^H}{\|\mathbf{h}_{S,R}\|}. \tag{4}$$

Thus, the received signals at the destination and the eavesdropper are given by

$$y_D = \sqrt{P_R \alpha_{R,D}}\mathbf{h}_{R,D}^H \mathbf{r}^{AF} + n_D, \tag{5}$$

and

$$y_E = \sqrt{P_R \alpha_{R,E}}\mathbf{h}_{R,E}^H \mathbf{r}^{AF} + n_E, \tag{6}$$

respectively, where P_R is the transmit power of the relay, n_D and n_E are the additive Gaussian white noises with zero mean and unit variance at the destination and the eavesdropper.

Since there is no knowledge of the eavesdropper channel at the source and the relay, it is impossible to provide a steady secrecy rate over all realizations of the fading channels. In this paper, we take the secrecy outage capacity C_{SOC} as the performance metric, which is defined as the maximum available rate under the condition that the outage probability that the real transmission rate surpasses the secrecy rate is equal to a given value ε, namely

$$P_r(C_{SOC} > C_D - C_E) = \varepsilon, \tag{7}$$

where C_D and C_E are the legitimate and the eavesdropper channel rates, respectively.

Note that C_{SOC} is not an decreasing function of P_R, since both C_D and C_E increase as P_R adds. Then, it makes sense to select an optimal P_R. The focus of this paper is on the optimal power allocation at the relay, so as to maximize the secrecy outage capacity for a given outage probability.

III. Optimal Power Allocation

In this section, we first analyze the condition that the secrecy outage capacity is positive, prove the existence of one and only one optimal power, and then design an optimal power allocation scheme for the relay. Finally, we present the asymptotic characteristics of the secrecy outage capacity.

Note that accurate performance analysis is the basis of power allocation. Prior to designing the optimal power allocation scheme, we first reveal the relation between the secrecy outage capacity and the transmit power. Based on the received signals in (3) and (4), the signal-to-noise ratio (SNR) at the destination and the eavesdropper can be expressed as

$$\gamma_D = \frac{P_S P_R \alpha_{S,R}\alpha_{R,D}|\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^2}{P_R \alpha_{R,D}|\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}|^2 + \|\hat{\mathbf{h}}_{R,D}\|^2 (P_S \alpha_{S,R}\|\mathbf{h}_{S,R}\|^2 + 1)}, \tag{8}$$

and

$$\gamma_E = \frac{P_S P_R \alpha_{S,R}\alpha_{R,E}|\mathbf{h}_{R,E}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^2}{P_R \alpha_{R,E}|\mathbf{h}_{R,E}^H \hat{\mathbf{h}}_{R,D}|^2 + \|\hat{\mathbf{h}}_{R,D}\|^2 (P_S \alpha_{S,R}\|\mathbf{h}_{S,R}\|^2 + 1)}. \tag{9}$$

Then, the legitimate and the eavesdropper channel rates are given by $C_D = W\log_2(1+\gamma_D)$ and $C_E = W\log_2(1+\gamma_E)$ respectively, where W is a half of the spectral bandwidth, since a complete transmission requires two time slots. Thus, for the secrecy outage capacity, we have the follow lemma:

Lemma 1: For a given outage probability by ε, the secrecy outage capacity of an LS-MIMO relaying system with imperfect CSI can be expressed as $C_{SOC} = W\log_2\left(1+\frac{P_S P_R \alpha_{S,R}\alpha_{R,D}\rho N_R^2}{P_R\alpha_{R,D}\rho N_R + P_S\alpha_{S,R}N_R+1}\right) - W\log_2\left(1+\frac{P_S P_R \alpha_{S,R}\alpha_{R,E} N_R \ln\varepsilon}{P_R\alpha_{R,E}\ln\varepsilon - P_S\alpha_{S,R}N_R} - 1\right)$.

Proof: The secrecy outage capacity can be obtained based on (7) by making use of the property of channel hardening in LS-MIMO systems [12]. We omit the proof, and the detail can be referred to our previous work [10]. ■

A. Positiveness

It is worth pointing out that the secrecy outage capacity may be negative or zero from a pure mathematical view. Therefore, it makes sense to find the condition that the positive secrecy outage capacity exists.

Let $\rho\alpha_{R,D}N_R = A$, $-\alpha_{R,E}\ln\varepsilon = A\cdot r_{gl}$, $P_S\alpha_{S,R}N_R = B$, where $r_l = \frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}N_R}$ is defined as the relative distance-dependent path loss. Then, the secrecy outage capacity can be rewritten as

$$\begin{aligned} C_{SOC} &= W\log_2\left(1+\frac{P_R AB}{P_R A + B + 1}\right) \\ &\quad - W\log_2\left(1+\frac{P_R ABr_l}{P_R Ar_l + B + 1}\right). \end{aligned} \tag{10}$$

Observing the secrecy outage capacity in (10), we get the following theorem:

Theorem 1: If and only if $0 < r_l < 1$, the secrecy outage capacity in an LS-MIMO relaying system in presence of imperfect CSI is positive.

Proof: Please refer to Appendix I. ■

Remarks: It is known that from Theorem 1, $0 < r_l < 1$ is a precondition for power allocation in such an LS-MIMO relaying system. Given channel conditions and outage probability, there is a constraint on the minimum number of antennas at the relay in order to fulfill $0 < r_l < 1$. Then, we have the following proposition:

Proposition 1: The number of antennas N_R at the relay must be greater than $\frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}}$.

Note that even with a stringent requirement on the outage probability, $\frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}}$ can be always met by adding the antennas, which is an advantage of an LS-MIMO relaying system. In what follows, we only consider the case of $0 < r_l < 1$.

B. Existence and Uniqueness

As shown in (10), the secrecy outage capacity is not an increasing function of P_R. Then, there may be an optimal power for the relay in the sense of maximizing the secrecy outage capacity. In this subsection, we aim to prove that the optimal power exists and is unique.

Prior to seeking the optimal power, we first check two extreme cases of P_R. On the one hand, if P_R is large enough, the terms $B+1$ in (10) is negligible, so the secrecy outage capacity is reduced as $C_{SOC} = W\log_2\left(1+\frac{P_R AB}{P_R A}\right) - W\log_2\left(1+\frac{P_R ABr_l}{P_R Ar_l}\right) = 0$. In other words, when P_R is very large, the SNRs at the destination and the eavesdropper asymptotically approach the same value. Thus, the secrecy outage capacity becomes zero. On the other hand, when P_R tends to zero, the secrecy outage capacity is equal to $C_{SOC} = W\log_2\left(1+\frac{0}{B+1}\right) - W\log_2\left(1+\frac{0}{B+1}\right) = 0$. Under this situation, both the rates of legitimate and eavesdropper channels tend to zero, and thus the secrecy outage capacity is also zero.

According to Theorem 1, the secrecy outage probability is positive when $0 < r_l < 1$, so the maximum secrecy outage capacity must appear at medium P_R regime. Then, we get the following theorem:

Theorem 2: From the perspective of maximizing the secrecy outage capacity, the optimal power at the relay in an LS-MIMO relaying system exists and is unique, once the relative distance-dependent path loss r_l is less than 1.

Proof: Please refer to Appendix II. ■

C. Optimal Power Allocation

From Theorem 2, it is known that as long as $0 < r_l < 1$, there is always a unique optimal power. In other words, if the relay applies the optimal power, the LS-MIMO relaying system gets the maximum secrecy outage capacity. Then, we have the following theorem:

Theorem 3: When the relay uses the power $P_R^\star = \sqrt{\frac{P_S\alpha_{S,R}N_R+1}{-\alpha_{R,E}\rho\alpha_{R,D}N_R\ln\varepsilon}}$, the LS-MIMO relaying system gets the maximum secrecy outage capacity, which is given by $C_{SOC}^{\max} = W\log_2\left(1+\frac{P_S\alpha_{S,R}N_R}{1+\sqrt{\frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}N_R}}(1+P_S\alpha_{S,R}N_R)}\right) -$

$$W \log_2 \left(1 + \frac{P_S \alpha_{S,R} N_R}{1+\sqrt{\frac{-\rho \alpha_{R,D} N_R}{\alpha_{R,E} \ln \varepsilon}(1+P_S \alpha_{S,R} N_R)}} \right).$$

Proof: Substituting the optimal power P_R in (14) into C_{SOC} in (10), we can derive the maximum secrecy outage capacity. ■

Remarks: The optimal power at the relay $P_R^\star$ is an increasing function of source transmit power P_S, source-relay path loss $\alpha_{S,R}$ and outage probability ε, and is a decreasing function of CSI accuracy ρ, relay-destination path loss $\alpha_{R,D}$ and relay-eavesdropper path loss $\alpha_{R,D}$. In addition, due to $r_l = \frac{-\alpha_{R,E} \ln \varepsilon}{\rho \alpha_{R,D} N_R} < 1$, the maximum secrecy outage capacity is an increasing function of P_S, $\alpha_{S,R}$, $\alpha_{R,D}$, ε, N_R and ρ, and is a decreasing function of $\alpha_{R,E}$.

D. Asymptotic Characteristic

As analyzed above, the optimal power at the relay $P_R^\star$ is an increasing function of the power at the source P_S. Next, we carry out asymptotic analysis to P_S and get the following theorem:

Theorem 4: At the low P_S regime, the optimal power $P_R^\star$ and the maximum secrecy outage capacity $C_{SOC}^{\max}$ tend to zero. In the high P_S region, the maximum secrecy outage capacity will be saturated and is independent of P_S.

Proof: Please refer to Appendix III. ■

As P_S approaches zero, the source does not transmit any information to the relay in the first slot, so the maximum secrecy outage capacity tends to zero. While P_S is sufficiently large, the forward noise at the relay is also amplified, and thus the secrecy outage capacity is saturated and is independent of P_S and P_R.

IV. Simulation Results

To examine the effectiveness of the proposed optimal power allocation scheme for the AF LS-MIMO relaying system, we present several simulation results in the following scenarios: we set $N_R = 100$, $W = 10$KHz, $\rho = 0.9$ and $\varepsilon = 0.01$. We assume that the relay is in the middle of the source and the destination. For convenience, we normalize the pass loss as $\alpha_{S,R} = \alpha_{R,D} = 1$ and use $\alpha_{S,E}$ to denote the relative path loss. Specifically, $\alpha_{R,E} > 1$ means the eavesdropper is closer to the relay than the destination. We use $\text{SNR}_S = 10 \log_{10} P_S$ and $\text{SNR}_R = 10 \log_{10} P_R$ to represent the transmit signal-to-noise ratio (SNR) in dB at the source and the relay, respectively.

First, we show the impact of r_l on the secrecy outage capacity with $\text{SNR}_R = 20$dB. As seen in Fig.2, the positive secrecy outage capacity exists only when $0 < r_l < 1$, which confirms the claims in Theorem 1. Given a r_l, the secrecy outage capacity increases gradually as P_S adds. However, the performance loss by reducing P_S from 30dB to 20dB is smaller than that by reducing P_S from 20dB to 10dB. This is because in the large P_S region, the secrecy outage capacity tends to be saturated.

Second, we validate the existence and uniqueness of the optimal power $P_R^\star$. As showed in Fig.3, the secrecy outage

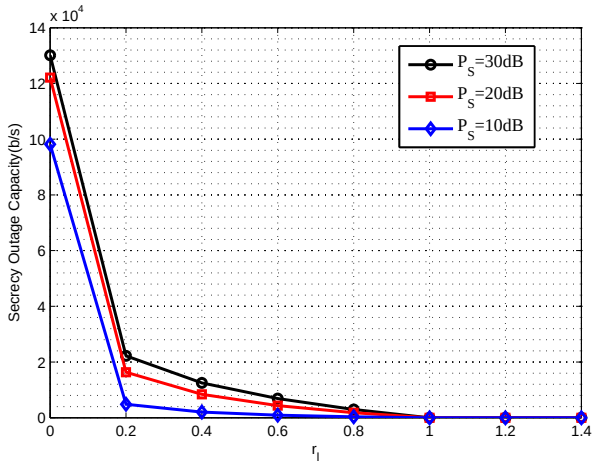

Fig. 2. Secrecy outage capacity with different relative distance-dependent path losses.

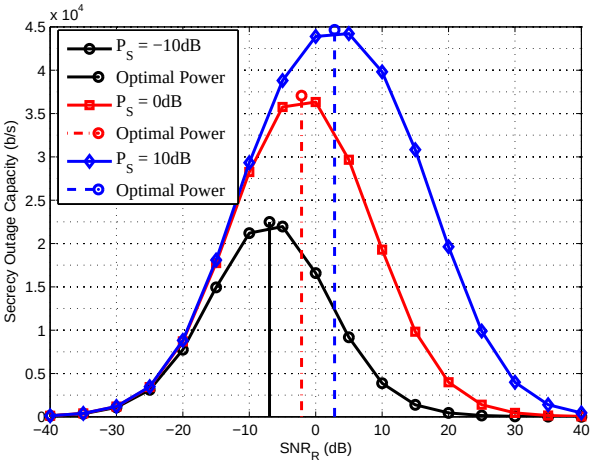

Fig. 3. Secrecy capacity with different SNR_R.

capacity approaches zero both when P_S tends to zero and infinity, and the unique optimal power associated to the maximum secrecy outage capacity appears in the medium region of P_S. Furthermore, it is found that both $P_R^\star$ and $C_{SOC}^{\max}$ improves as P_S increases, which confirms our theoretical claims again.

Then, we testify the accuracy of the theoretical expression of the maximum secrecy outage capacity with $\text{SNR}_S = 10$dB. As seen in Fig.4, the theorem results are well consistent with the simulations in the whole $\alpha_{R,E}$ region with different outage probability requirements, which proves the high accuracy of the derived performance expression. As claimed above, given an outage probability bound by ε, as $\alpha_{R,E}$ increases, the maximum outage secrecy capacity decreases. This is because the interception capability of the eavesdropper enhances when the interception distance becomes small. What's more, given a $\alpha_{R,E}$, the maximum secrecy outage capacity increases with the increase of ε.

Next, we show the performance gain of the proposed optimal power allocation scheme compared with a fixed power

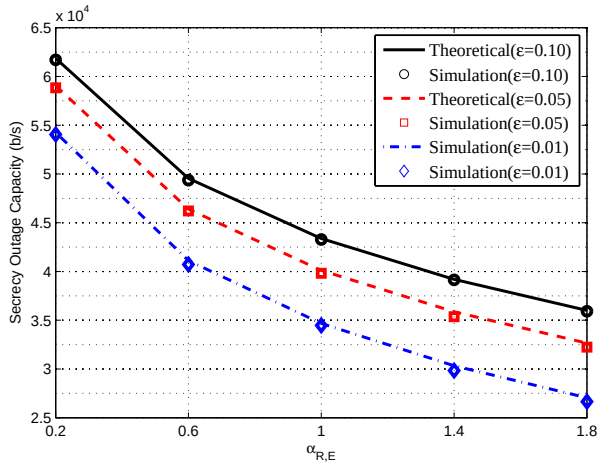

Fig. 4. Comparison of theoretical and simulation results.

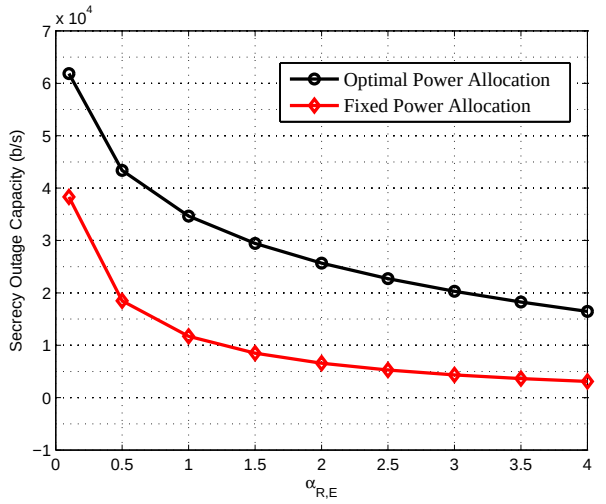

Fig. 5. Performance gain with different $\alpha_{R,E}$.

allocation scheme with $\text{SNR}_S = 10$dB. It is worth pointing out the fixed scheme uses a fixed power $P_R = 20$dB regardless of channel conditions and system parameters. As seen in Fig.5, the optimal power allocation scheme performs better than the fixed scheme. Even with a large $\alpha_{R,E}$, such as $\alpha_{R,E} = 4$, namely short-distance interception, the optimal scheme can still achieve a high performance gain, which proves the effectiveness of the proposed scheme.

Finally, we show the effect of P_S on the maximum secrecy outage capacity. As seen in Fig.6, when P_S tends to zero, the maximum secrecy outage capacity with different $\alpha_{R,E}$ approaches zero. In the large P_S region, the maximum secrecy outage capacity will be saturated for a given ε, which proves the Theorem 3 again. Consistent with our theoretical analysis, the performance ceiling is an decreasing function of $\alpha_{R,E}$.

V. Conclusion

This paper focus on the optimal power allocation for a secure AF LS-MIMO relaying system with imperfect CSI.

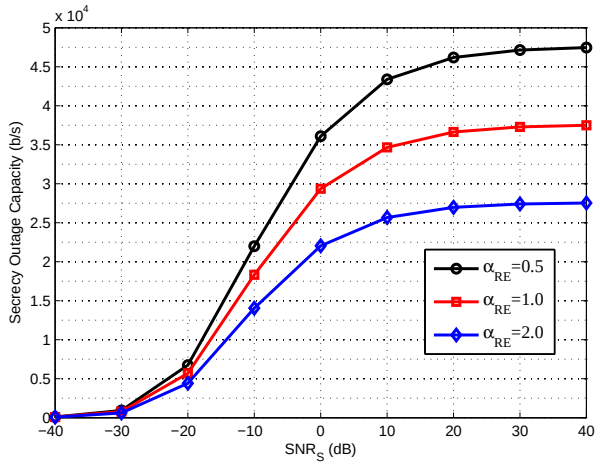

Fig. 6. Maximum secrecy capacity with different SNR_S.

We present the condition that the secrecy outage capacity is positive, prove the existence and uniqueness of the optimal power at the relay, and propose an optimal power allocation scheme. Moreover, we reveal the asymptotic characteristics of the maximum secrecy outage capacity in cases of low and high source transmit powers.

Appendix A
Proof of Theorem 1

To get the condition that the secrecy outage capacity is positive, we first rewrite (10) as

$$\begin{aligned} C_{SOC} &= W\log_2\left(1+\frac{P_R AB}{P_R A+B+1}\right) \\ &\quad -W\log_2\left(1+\frac{P_R AB}{P_R A+\frac{B+1}{r_l}}\right). \end{aligned} \tag{11}$$

Examining (11), it is found that if and only if $0 < r_l < 1$, the secrecy outage capacity is positive. According to the definition of the relative distance-dependent path loss $r_l = \frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}N_R}$, $0 < r_l < 1$ is equivalent to the following condition:

$$N_R > \frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}}. \tag{12}$$

In other words, only when $N_R > \frac{-\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}}$, the secrecy outage capacity is positive. Therefore, we get Theorem 1 and Proposition 1.

Appendix B
Proof of Theorem 2

At first, we take derivative of (10) with respect to P_R, which is given by (13) at the top of the next page. Let $C'_{soc} = 0$, we get two solutions

$$P_R = \frac{1}{Ar_l}\sqrt{r_l(B+1)}, \tag{14}$$

and

$$P_R = -\frac{1}{Ar_l}\sqrt{r_l(B+1)}. \tag{15}$$

$$C'_{soc} = \frac{W}{\ln 2} B(1+B) \left(\frac{A}{(P_R A + B + 1)^2 + P_R AB(P_R A + B + 1)} - \frac{Ar_l}{(P_R Ar_l + B + 1)^2 + P_R ABr_l(P_R Ar_l + B + 1)} \right). \quad (13)$$

Considering $P_R > 0$, (14) is the unique optimal solution in this case. What's more, when $P_R < \frac{1}{Ar_l}\sqrt{r_l(B+1)}$, we have $C'_{soc} > 0$. Otherwise, if $P_R > \frac{1}{Ar_l}\sqrt{r_l(B+1)}$, we have $C'_{soc} < 0$. Specifically, C_{SOC} improves as P_R increases in the region from 0 to $\frac{1}{Ar_l}\sqrt{r_l(B+1)}$, while C_{SOC} decreases as P_R increases in the region from $\frac{1}{Ar_l}\sqrt{r_l(B+1)}$ to infinity. Only when $P_R = \frac{1}{Ar_l}\sqrt{r_l(B+1)}$, the secrecy outage capacity achieves the maximum value. In other words, the optimal solution exists and is unique. Hence, we get the Theorem 2.

APPENDIX C
PROOF OF THEOREM 4

According to Theorem 3, the maximum secrecy outage capacity can be expressed as

$$\begin{aligned} C_{SOC}^{\max} &= W\log_2\left(1+\frac{\sqrt{r_l(B+1)}B}{\sqrt{r_l(B+1)}+r_l(B+1)}\right) \\ &\quad -W\log_2\left(1+\frac{\sqrt{r_l(B+1)}B}{\sqrt{r_l(B+1)}+(B+1)}\right), \\ &= W\log_2\left(1+\frac{1}{\frac{1}{B}+\sqrt{r_l(\frac{1}{B}+\frac{1}{B^2})}}\right) \\ &\quad -W\log_2\left(1+\frac{1}{\frac{1}{B}+\sqrt{\frac{1}{r_l}(\frac{1}{B}+\frac{1}{B^2})}}\right). \quad (16) \end{aligned}$$

Intuitively, B tends to zero as P_S approaches zero. Then, $\frac{1}{\frac{1}{B}+\sqrt{r_l(\frac{1}{B}+\frac{1}{B^2})}}$ and $\frac{1}{\frac{1}{B}+\sqrt{\frac{1}{r_l}(\frac{1}{B}+\frac{1}{B^2})}}$ in (16) becomes zero. Thus, we have $C_{SOC}^{\max} = 0$. On the other hand, if P_S is large enough, B is also very large. Therefore, the maximum secrecy outage capacity is transformed as

$$\begin{aligned} C_{SOC}^{\max} &= W\log_2\left(1+\frac{\sqrt{r_l(B+1)}B}{\sqrt{r_l(B+1)}+r_l(B+1)}\right) \\ &\quad -W\log_2\left(1+\frac{\sqrt{r_l(B+1)}B}{\sqrt{r_l(B+1)}+(B+1)}\right), \\ &= W\log_2\left(1+\frac{B}{1+\sqrt{r_l(B+1)}}\right) \\ &\quad -W\log_2\left(1+\frac{B}{1+\sqrt{\frac{B+1}{r_l}}}\right), \\ &\approx W\log_2\left(1+\frac{B}{\sqrt{r_l(B+1)}}\right) \\ &\quad -W\log_2\left(1+\frac{B}{\sqrt{\frac{B+1}{r_l}}}\right) \quad (17) \\ &\approx W\log_2\left(1+\frac{B}{\sqrt{r_l B}}\right) - W\log_2\left(1+\frac{B}{\sqrt{\frac{B}{r_l}}}\right) \quad (18) \\ &= W\log_2\left(1+\sqrt{\frac{B}{r_l}}\right) - W\log_2\left(1+\sqrt{r_l B}\right), \\ &= W\log_2\left(\frac{\sqrt{\frac{B}{r_l}}}{\sqrt{r_l B}}\right), \\ &= W\log_2\left(\frac{1}{r_l}\right). \quad (19) \\ &= W\log_2\left(\frac{\rho\alpha_{R,D}N_R}{-\alpha_{R,E}\ln\varepsilon}\right), \quad (20) \end{aligned}$$

where (17) and (18) hold true because when B is big enough, the constant term "1" is negligible. Hence, we get the Theorem 3.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, Oct. 1975.

[3] P. K. Gopala, L. Lai, and H. El. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[4] J. Barros, and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, pp. 356-360, July 2006.

[5] T. T. Kim, and H. V. Poor, "On the Secure degree of freedom of relaying with half-duplex feedback," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 291-302, Jan. 2011.

[6] C. Jeong, I-M. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310-325, Jan. 2012.

[7] J. Huang, and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 39, no. 10, pp. 4871-4884, Oct. 2011.

[8] X. Chen, and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 503-506, Oct. 2013.

[9] H-M. Wang, M. Luo, X-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Proces. Lett.*, vol. 20, no. 1, pp. 39-42, Jan. 2013.

[10] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *Proc. IEEE ICC*, pp. 1-6, Jun. 2014.

[11] C. Jeong, and I-M. Kim, "Optimal power allocation for secure multi-carrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428-5442, Nov. 2011.

[12] B. M. Hochwald, T. L. Marzetta, and V. Tarokh, "Multiple-antenna channel hardening and its implications for rate-feedback and scheduling," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893-1909, Sept. 2004.